Update 20. August 2026

Technischer Sicherheitsvorfall im Juli 2026 am IDOS

Wir sind wieder per E-Mail erreichbar.

E-Mails, die **seit Montagnachmittag 17. August** gesendet wurden, werden **zwischengespeichert** und können **seit Mittwoch 19. August** wieder von unseren Mitarbeitenden **gelesen und bearbeitet** werden.

E-Mails, die im Zeitraum vom **27. Juli 2026 bis Montagvormittag 17. August 2026** an uns gesendet wurden, haben uns **nicht erreicht**. Sie wurden auch **nicht zwischengespeichert**.

Die Überarbeitung und Absicherung der restlichen IT-Infrastruktur dauert an.

Technischer Sicherheitsvorfall im Juli 2026

Im Juli 2026 erfolgte ein Angriff auf eine Netzwerkkomponente des IDOS, über die **versucht wurde, auf interne Systeme zuzugreifen**.

Sowohl die unmittelbar nach der Entdeckung des Vorfalls gemeinsam mit externen IT-Sicherheitsspezialisten begonnen Analysen als auch die Überarbeitung der Absicherung der gesamten IT-Infrastruktur des IDOS dauern an. Die betroffene Netzwerkkomponente, die als Einfallstor identifiziert wurde, ist inzwischen **vollständig erneuert**.

Die seit der Stellungnahme vom 6. August 2026 fortgeführten Analysen bestätigen, dass alle dem Angriff zuzuordnenden Zugriffsversuche auf interne Systeme gescheitert sind, es gibt weiterhin **keine Hinweise auf Kompromittierung, auf einen Zugriff auf gespeicherte Daten oder auf einen Datenabfluss. Es wurden keine Daten verschlüsselt durch Ransomware.**

Vielen Dank für Ihr Verständnis.

Prof. Dr. Anna-Katharina Hornidge, Dr. Axel Berger, Margret Heyen

Update, 20 August 2026

Technical security incident at IDOS in July 2026

We are again reachable by email.

Emails sent **since Monday afternoon, 17 August**, have been **temporarily stored** and **are available** for our staff to read and process again since **Wednesday, 19 August.**

Emails sent to us **between 27 July 2026 and Monday morning, 17 August 2026 did not reach us**. **Nor** were they **temporarily stored**.

In addition, the work to further review and secure the remainder of the IT infrastructure continues.

Technical security incident in July 2026

In July 2026, an attack was carried out on a network component belonging to IDOS, through which an **attempt was made to gain access to internal systems**.

Both the investigations, which began immediately after the incident was discovered in collaboration with external IT security specialists, and the review of the security measures for IDOS entire IT infrastructure are ongoing. The affected network component, which was identified as the point of entry, **has since been completely replaced**.

The analyses, which have continued since the Statement of 6 August, confirm that all attempts to access internal systems attributable to the attack have failed; there is still **no evidence of a breach, of access to stored data or of a data leak. No data has been encrypted by ransomware.**

Thank you for your understanding.

Prof. Dr. Anna-Katharina Hornidge, Dr. Axel Berger, Margret Heyen